



CIPA Filter

6/16/2006 - 5.0.246

1. Introduction

CIPAFilter is a network hardware appliance solution that combines unique development with great tech support and low pricing, for a fully polished and highly competitive solution designed to genuinely help school district Technology Coordinators and computer network administrators.

DerbyTech's philosophy is to provide a cutting edge, well rounded, and aggressive network control solution to meet your current and future needs, commit to keeping your platform up to date, and to provide support far above and beyond simple problem solving. We believe our philosophy is what sets our product firmly apart from our competitors. Our technicians will talk you through installation every step of the way. We will advise you on what features are a good fit for your organization and help you implement them. We will protect your return on investment by assuring that you can always easily upgrade to our latest platforms, often at no cost. And of course, we will help you solve any problems you encounter with our product, even when it's caused by a third party agent, software package, or network problem.

CIPAFilter provides

- Advanced Router/Firewall
- Content Filter and Web Caching Engine
- Complete Virus Protection
- Anti-Spam and E-mail Virus Protection
- Web Authentication & Proxy Services
- Bandwidth Monitoring and Management
- Web Usage Reporting
- VPN & Advanced Routing Capabilities
- E-mail Archiving

This reference will provide the information necessary for an experienced network technician to configure and operate these services. However, this manual is not intended to replace our excellent and unlimited technical support. Many users never even log into the CIPAFilter interface, other than for brief monitoring of logs and services. Please feel free to contact us to have a technician walk you through and consult on the best method of integrating CIPAFilter on your network.

2. Table of Contents

Table of Contents

1. Introduction	4	8. IPSEC Configuration	27
2. Table of Contents	6	Field Descriptions	28
3. Interface Conventions	9	Procedure for creating a RSA tunnel	30
4. Technical Support	10	Procedure for Creating a X509 VPN tunnel	31
5. Installation	11	9. Statefull Firewall and Layer 7 Filtering	33
As a replacement for your firewall	12	TCP/UDP Firewall	33
As a Bridge	13	Example Firewall Configurations	35
As a Proxy Server and Mail Relay Server	14	ICMP Firewall	37
Virus Scanning	15	10. Web Proxy	39
6. IP and Interfaces Configuration	17	Field Descriptions	40
Dot Notation to CIDR Notation Translation Table	18	E-mail Services	45
Field Descriptions	20		
7. Routing Configuration	23		
Field Descriptions	24		

11. White list/Black list	51	18. Statistics	60
12. Port Forwarding	53	Bandwidth Usage	60
13. Bandwidth Control	55	Anti-Spam Statistics	60
14. DHCP Server	56	Anti-Virus Log	61
15. User Manager	57	Web Usage Reporting	61
16. Config Save and Restore	58	19. Appendix I: Dot Notation to CIDR Notation Translation Table	62
17. Remote Console	59	20. Appendix II: POSIX Regular Expressions	63

3. Interface Conventions

If an option name in the web based user interface is highlighted with a blue link, that indicates the link will bring up a help document describing the option.

Clicking a "Save" button will cause the configuration options on any particular page to be saved but not activated. "Save and Apply" will cause the configuration options to be saved and activated. If there is no "Save and Apply" option on any given page, that means the firewall must be restarted to activate the changes.

4. Technical Support

DerbyTech is committed to excellence and providing industry-leading support and consulting. Each CIPAFilter includes unlimited support and free installation assistance in order to ensure a successful implementation of the product on your network. Feel free to call any of our trained technicians with questions or concerns.

Phone Support

Call 800.24.DERBY x3000 (opt. 1,2),
Monday - Friday, 8am to 5pm. CST

In case of an emergency and after-hours support, choose opt. 1, 3 to get forwarded to a support hotline. You may leave a message for a technician.

Online Support

Check out our FAQ <http://cipafilter.com/faq/>
or email the support team at
support@cipafilter.com

Feedback

Your feedback is important! We encourage ideas, comments and questions regarding future development of CIPAFilter. If you have a feature you would like to see implemented, or a comment about our support or technology, e-mail us at feedback@cipafilter.com. Your participation is greatly appreciated.

5. Installation

In most cases you will want to consult with DerbyTech to decide what way the firewall can best be installed to meet your needs. A full over the phone consultation during installation is included in the standard one year maintenance and service agreement that comes with your firewall.

CIPAFilter is usually installed one of four ways, replacing your existing firewall, a bridge spliced into the link between your existing firewall and your switch bank, or as a proxy server/mail relay server.

Of the four ways that CIPAFilter is usually installed, installation as a bridge is the easiest. Installation replacing your existing firewall is most recommended.

The CIPAFilter ships with 10.1.2.3/8 assigned to it's first ethernet interface and 192.168.0.1/24 assigned to it's second. If your network does not use one of these IP addresses you can simply assign an IP like 10.1.2.1/8 (netmask 255.0.0.0) to your workstation and plug the CIPAFilter into your hub or switch.

If your network does use these IP addresses plugging your CIPAFilter in without taking the proper precautions could cause loss of Internet access or other problems. If you're not sure call us for assistance.

Open up <https://10.1.2.3> in your web browser to begin configuration. Default user name is root and default password is derby. The password can be changed on the "User Manager" page.

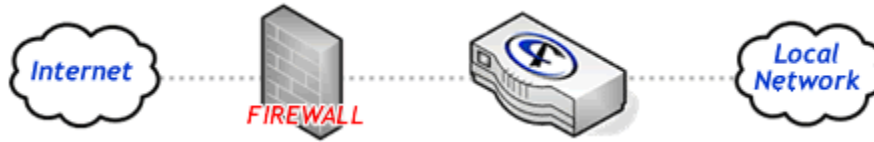
As a replacement for your firewall

Often you will find the best way to install CIPAFirewall is as a replacement for your current firewall. CIPAFirewall is a top of the line firewall and implements virtually all the functionality of other routing systems. In this case you would configure CIPAFirewall with the IP addresses, routes and NAT settings currently on your firewall, and then replace your current firewall.



As a Bridge

The easiest way install CIPAFilter is as a bridge, simply unplug your existing firewall from your switch bank, connect CIPAFilter to that port on your firewall via a cross over cable, then connect the cable that was plugged into your firewall to the other port on CIPAFilter. Check "Interface Bridging" on the "IP And Interfaces" page on the web based interface. Your network should now operate normally, and you can activate CIPAFilter features one by one as you're ready to implement them.



As a Proxy Server and Mail Relay Server

Many features of the CIPAFilter can be used simply by assigning it an IP address on your network and connecting it like any other server.

Disadvantages:

- No transparent proxy.
- No POP3 Virus scanning.
- Firewall ineffective.
- You will often need to add firewall rules to your existing firewall to force users to use the proxy server in order to make CIPAFilter effective at protecting your network.
- Bandwidth control only effective for Internet traffic working through the proxy server.
- Bandwidth usage may not be able to monitor all traffic on your network.



Virus Scanning

CIPAFilter's Virus scanning is easy to setup but please be certain to attempt a test virus transmission through each protocol you intend to protect to insure proper setup after installation. You can download a "test" virus from <http://eicar.com/>. Eicar is a text string "placebo" that all virus detectors are programmed to detect as a virus. It is harmless, and only a few dozen bytes long.

SMTP antivirus is the primary method for E-mail protection and requires that your MX record points to the CIPAFilter or SMTP port 25 is forwarded to CIPAFilter from your MX. Your mail can then be forwarded on to your internal mail server with the "Mail Routing" options on the "Mail and Web Proxy" page.

POP3 virus scanning is automatic and will scan all POP3 traffic passing through the firewall. This feature is not designed to be the primary mail anti-virus method, but only to scan those users have may also have external e-mail accounts that they access from within your organization via POP3. If your network is large and all your normal e-mail traffic is going to pass through CIPAFilter as POP3 please make special arrangements with Tech Support.

HTTP/FTP virus scanning requires web proxy to be activated and functioning in order to operate. HTTP and FTP anti-virus will work in both transparent and proxy server modes.

6. IP and Interfaces Configuration

Each interface has a primary IP address as well as optional additional secondary IP addresses. An IP address of 0.0.0.0/0 indicates that the interface is to be left unconfigured. Secondary IP addresses can be assigned to an interface by clicking "Add IP" near the bottom of each interface section.

IP addresses are specified CIDR Notation, an Address/Subnet bits format. The subnet bits refers to the number of bits that are set in binary in the subnet mask from the left hand side. For example, a subnet mask of 255.0.0.0 in binary has 8 bits set from the left hand side. So, 10.0.0.25 with a subnet mask of 255.0.0.0 translates to 10.0.0.25/8 in CIDR Notation. You can use the following table to translate some common subnet masks (Dot notation) into CIDR Notation.

Dot Notation to CIDR Notation Translation Table

Subnet Mask	Subnet Bits	IP Addresses
255.0.0.0	/8	16,581,375
255.255.0.0	/16	65,025
255.255.255.0	/24	256
255.255.255.128	/25	128
255.255.255.192	/26	64
255.255.255.224	/27	32
255.255.255.240	/28	16
255.255.255.248	/29	8
255.255.255.252	/30	4
255.255.255.254	/31	2
255.255.255.255	/32	1

NAT (Network Address Translation) is a system whereas private IP addresses (Such as 10.0.0.0/8 and 192.168.0.1/24) are mapped onto a public Internet IP from your ISP. To NAT a subnet of private IP's click the NAT check box next to the private IP subnet and click the "Primary Internet Connection" radio button on the interface using your ISP assigned public IP. All traffic from the NAT'd subnet will now be mapped to the primary IP address of the "Primary Internet Connection" device.

Settings like hostname and timezone can also be set on this page. If you are using the mail features of CIPAFILTER make sure the hostname and domain are correct. Make sure the "hostname.domain" combination resolves to an IP address on the CIPAFILTER and that the IP address reverses properly back to "hostname.domain". This is important because many mail servers will refuse to trade e-mail with your CIPAFILTER if this is not done.

Field Descriptions

Interface Bridging

Clicking this checkbox will cause CIPAFilter to become a bridge, bridging all its ethernet interfaces together into one logical interface. In this configuration CIPAFilter acts like a switch. [Installing CIPAFilter this way may require the restarting of any CISCO routers on the subnet to clear their ARP cache.](#) Any IP addresses you wish to configure CIPAFilter with for management can be applied to any interface if this box is checked.

SMB Domain

The SMB Domain is the Windows NT or Active Directory Domain name served by your PDC or AD Server. The CIPAFilter will authenticate against this domain when using the "Windows Active Directory" authentication method to authenticate proxy users.

Primary Internet Connection

The interface closest to the Internet should be chosen as your "Primary Internet Connection". This is important if you turn on NAT (Network Address Translation) on any of your other subnets. If a subnet is being NAT'd, all packets coming from it through the router are translated to appear as if they are coming from the IP you designate as the "Primary Internet Connection".

Network Address Translation

Network address translation or NAT is used to allow a group of machines with private IP addresses like 10.0.0.0/8 or 192.168.0.0/24 to access the Internet. Packets flowing from any subnet with NAT checked will have their source address modified to reflect the IP address of your [Primary Internet Connection](#) before continuing on. Packets coming back to the [Primary Internet Connection](#) will then be sorted and passed on to their real destinations. You only have to check NAT on a single IP from each subnet. For example, if you have five IP's on the 10.0.0.0/8 subnet, you only need to turn NAT on on any one of them to NAT all traffic from the 10.0.0.0/8 subnet.

OSPF Metric and Area

These are OSPF settings. They are only important if you have deployed dynamic routing on your network. Default metric is 500. Default area is 0. See the routing section of this manual and contact DerbyTech if you wish to deploy dynamic routing on your network and need more information.

7. Routing Configuration

The CIPAFilter is a fully featured router capable of replacing the functionality of your existing routers. Modules are available for T1, 802.11a/b/g and Ethernet protocols.

Most customers will not need to reconfigure any features on this page. CIPAFilter will automatically route between any subnets specified on it's interface page.

OSPF and BGP should be left off, unless you are deploying dynamic routing. If you do intend to use dynamic routing, please contact Tech Support for assistance. Keep in mind that CIPAFilter uses only MD5 OSPF key encryption. CIPAFilter also ignores the default gateway entered on the "IP and Interfaces" page if OSPF is activated unless "Advertise default route" is selected. CIPAFilter advertises all static routes by default back into the OSPF cloud.

The watchdog option causes CIPAFilter to restart if it loses connectivity with it's default gateway for more than 20 minutes. CIPAFilter measures it's connectivity with a ping once per minute, so if your ISP has configured your default gateway to drop pings this option should be unchecked.

BGP can only be configured manually from the console.

Field Descriptions

OSPF

OSPF is a dynamic routing protocol. Unless you have already deployed it on your network just leave this unchecked. CIPAFilter's implementation of OSPF uses only message digest authentication, and advertises all static routes and all local interface subnets back into the OSPF cloud. Static routes are advertised with a metric of 5,000. The default gateway set on the "IP and Interfaces" page is ignored unless [Advertise Default Route](#) is checked. If [Advertise Default Route](#) is checked the default gateway is advertised with a metric of 30,000.

BGP

BGP is a dynamic routing protocol used to advertise IP ranges to upstream ISP's on most networks. If your network uses BGP please contact tech support. This feature can only be configured from the console.

Advertise Default Route

When OSPF is active by default CIPAFilter ignores the default gateway from the "IP and Interfaces" page. If this option is checked CIPAFilter will advertise the default route back into the OSPF cloud and consider it for routing purposes. The default gateway is advertised with a metric of 30,000.

Default Gateway Watchdog

If CIPAFILTER loses connectivity with its default gateway for more than 20 minutes this option causes it to restart. CIPAFILTER measures its connectivity with a ping, so if your ISP has configured your default gateway to drop pings this option should be unchecked.

OSPF Key

The message digest key CIPAFILTER uses to authenticate itself to the other routers in your OSPF cloud.

NAT

If the nat checkbox next to a route is checked, all traffic coming from this subnet will automatically be source nat'd to the first IP on the Primary Internet Connection.

8. IPSEC Configuration

VPN tunnels are tricky normally, and IPSEC tunnels are even worse. Configuring tunnels between our routers isn't too hard, but configuring a Windows machine to be compatible with the GPL FreeSWAN IPSEC implementation we use is much more complicated if you've never done it before. We provide instructions here but we encourage our customers to allow us to help you through the process. Please feel free to call us and let us advise you on your design and talk you through the implementation.

There are two types of tunnels supported by our routers, X509 certificate tunnels included for Microsoft software compatibility and standard RSA tunnels. The X509 tunnels can do everything that the RSA tunnels do, but a [X509 tunnel requires you to acquire certificates from DerbyTech](#). A certificate is a digital document attesting to the identity of a computer or router that has been signed with DerbyTech's private key. These documents can be used by two machines to prove their identities to each other so an encrypted session can be established.

If your VPN is not working, call DerbyTech and we will troubleshoot it remotely for you.

Field Descriptions

My Subnet

This is the private subnet this router is making available to other routers and workstations through the VPN.

Connection Name

This is an arbitrary name given to the connection to remind you which one it is. Spaces and punctuation other than the dash are not allowed. Do not use a dash as the first character of the field.

Remote IP

IP address of the router or workstation at the other end of this tunnel. Use "%any" for a workstation or router with a dynamic IP address.

Remote Subnet

This is the private subnet the other router is making available to the clients behind this router. If the other end of this tunnel is just a workstation use "none".

Remote Name

For RSA tunnels only. This is the other router's name exactly as it appears on the "IP and Interfaces" page. The name is the hostname and domain together.

Example:

Hostname: mail

Domain: derbyworks.com

Remote Name: mail.derbyworks.com

Remote Subject

For X509 tunnels only. Paste the subject from the subject.txt file in the certificate from the Workstation into this field. Do not include "Subject:"

Remote SigKey

For RSA tunnels only. The sigkey of the remote router goes here. Obtain the sigkey by clicking "Display My Keys" on the remote router. The sigkey is the text after "leftsasigkey=" on the page that pops up. Do not include "leftsasigkey=" in the field.

Procedure for creating a RSA tunnel

Use these tunnels to connect 2 CIPAFilters.

1. Before you make your first tunnel you should "Reset Key Pairs" on both routers. Do this only once when you install your router, as any tunnels created before you reset the pairs will stop working and need to be recreated. If the router has been restarted recently resetting the key pairs can take quite some time as the router gathers entropy and might timeout. It is recommended to reset the key pairs after the router has been online over night or at least after a few hours of uptime.
2. Set "My Subnet" to the subnet the remote routers will be accessing.
3. Click "Add RSA Tunnel"
4. Set the connection name to something to help you remember where the connection is going. No spaces or punctuation other than the dash, and don't start the name with a dash.
5. Set the "Remote IP" to the IP address of the other router.
6. "Remote Name" is the name of the other router as it appears on the "IP and Interfaces" page. The name is the hostname and the domain name together: "hostname.domain"
7. "Remote Subnet" is the subnet you will be accessing on the remote router.
8. Paste the remote router's sigkey into the "Remote Sigkey" field. The remote router's sigkey can be determined by clicking "Display My Keys" on the remote router. The sigkey is the string of characters after "leftrsasigkey=" in the display. Do not include "leftrsasigkey=" when you paste the sigkey. The sigkey is changed when the keypairs are reset. If you reset the keypairs on the other router in the future you will have to copy and paste the new sigkey into this field.
9. Click save and apply.
10. Follow steps 2-9 on the other router and you should be able to verify ping connectivity in about 10 seconds or so.

Procedure for Creating a X509 VPN tunnel

Use these tunnels to connect a CIPAFILTER and a Windows XP Pro Workstation.

1. Acquire a new certificate from DerbyTech for your router and workstation at 1800-24DERBY. Please be advised that though the default certificate installed on your router will work, it is theoretically possible for another DerbyTech customer to lift the private part of the certificate from their router and use it to attack your encryption. Acquiring your own private router certificate is recommended for any encryption that rises above the casual level. In either case, a private certificate for your workstation is required.
2. Upload the certificate to the "Upload New Cert" field on the "IPSEC" page on your router and hit Save.
3. Unzip the Windows certificate file onto the hard drive of the workstation that needs to be configured.
4. Double-click or open up "ipsec.msc" in the unzipped folder.
5. Right-click on Personal (under certificates), go to All Tasks - Import...
6. Browse the unzipped folder and select "client.cert" then click next. The password is "derby". Click next until the import is successful.
7. Under New Certificates, drag "DerbyWorks" to the Trusted Roots Certificates folder on the left.
8. Copy "ipseccmd" from the uncompressed folder to systemroot\system32.
9. Go to the IPsec_config directory. Edit the ipsec.conf file, but be carefull to only change the things you are instructed to change by these instructions. Some fields in the file look like things that should be edited but they need to remain the same.
10. Enter the IP of the remote router or computer after "right=".
11. Enter the remote subnet (subnet/mask) behind the router or computer after "rightsubnet".
12. Save and close the file.

13. Add a X.509 Tunnel to the Ipsec configuration on the remote router.
14. Connection name is arbitrary, it is there to remind you what the connection is. Don't use spaces or punctuation other than the dash, and don't start a name with a dash. Set the "Remote IP" to "%any" for a client with a dynamic IP, and the subnet to "none" for a client without a subnet behind it.
15. Copy the subject line from the subject.txt file in the uncompressed directory into the Subject line on the new tunnel. Make sure there is no garbage symbols at the end of the line. Don't include the words "Subject:".
16. Set the "My Subnet" field at the top of the page to the subnet you wish the remote workstations to access.
17. Click Save and Apply on the page.
18. To initiate the VPN, run "ipsec" from the ipsec-config directory. "ipsec" will need to be rerun any time the workstation changes it's IP address. You should consider putting a shortcut on the desktop. Wait about 10 seconds and you should be able to verify ping connectivity to a device on the remote subnet.

9. Statefull Firewall and Layer 7 Filtering

TCP/UDP Firewall

A statefull firewall is far more secure and easier to use than your average firewall because it tracks all open connections, not just packets. With a normal firewall, if you wanted your clients to be able to access web servers on the Internet you'd have to allow any machine on the Internet to access all the high ports on any client. This is a vulnerability many worms and trojans have been written to exploit.

With a statefull firewall you specify how connections are to be made. For example, you can allow any client inside your network to make a connection to port 80 on any server outside. When that happens, only that server, and only from port 80, will be able to send packets back to the high port on your client that originated the connection.

In addition, CIPAFirewall's firewall allows you to match rules on layer 7 (Application layer) protocols like chat, peer to peer, or external proxy servers. Eliminating these applications from your network is as easy as selecting "Chat", "Peer to Peer", or "Proxy Bypass" from the protocol drop down and choosing REJECT from the action column.

The "Policy" of a firewall determines whether or not it normally drops or accepts connections that it doesn't have explicit rules for. Normally, you will leave the firewall policy set to "Accept", but if you are an expert and want to define exactly how and only how each client on your network can use the Internet you can use the "Drop" policy.

NOTE: Connections are only matched against the firewall when they are first opened. If you change the firewall already open connections will remain open even if the new firewall would have prohibited them. Also note that the firewall does not apply to CIPAFilter itself. CIPAFilter automatically adjusts it's own firewall based on the configuration of the system to assure proper operation.

Some Tips:

- ! can be used as "not" on subnets or ports.
- : can be used to denote port ranges, ex: 80:110 for 80-110.
- Accept allows the connection.
- Reject rejects the connection and sends an error message to the client.
- Drop loses all the packets and sends no error message back to the client.
- Do not use any spaces in the rules.
- The firewall is fully integrated with the port forwarding system. Make firewall rules using the actual private IP addresses of your internal servers, not the public IP address you are port forwarding to them from.

Example Firewall Configurations

<i>Accept/Reject</i>	<i>Protocol</i>	<i>Connections From</i>	<i>To</i>	<i>On Port</i>	<i>Result</i>
REJECT	TCP	10.0.0.14/32	0.0.0.0/0	80	Workstation with ip address 10.0.0.14 can't use the web.
REJECT	TCP	164.215.40.0/24	10.0.0.15/32	80	The firewall is fully integrated with the port forwarding system. This rule would reject anybody that tries to connect to port 80 on the internal web server 10.0.0.15 unless the client was on the 64.215.40.0/24 subnet.
REJECT	ALL	10.0.0.25/32	0.0.0.0/0	ALL	Keep 10.0.0.25 from making connections to the outside world.
REJECT	CHAT	10.1.1.0/24	0.0.0.0/0	ALL	Computers in the 10.1.1.0/24 subnet can not use Internet chat programs.

The firewall rules are interpreted top down, so the first rule that matches a connection will determine it's fate. For example:

Accept/Reject	Protocol	Connections From	To	On Port	Result
ACCEPT	TCP	208.20.191.0/24	10.0.0.15/32	80	Allows the 208.20.191.0/24 subnet to access the internal web server.
ACCEPT	TCP	64.215.40.0/24	10.0.0.15/32	80	Allows the 64.215.40.0/24 subnet to access the internal web server.
DROP	ALL	0.0.0.0/0	10.0.0.15/32	ALL	Drop all connections to the web server that have not already been accepted.
ACCEPT	Audio/Video	10.0.0.25/32	0.0.0.0/0	ALL	Allow 10.0.0.25 to receive audio and video traffic.
REJECT	Audio/Video	0.0.0.0/0	0.0.0.0/0	ALL	Rejects all other Audio/Video Traffic

The first 2 rules will allow machines on the 208.20.191.0/24 and the 64.215.40.0/24 subnet to access the internal web server at 10.0.0.15. However, they will only be able to access the web service on that server. All connections going to all other services or from other subnets will be dropped on the third rule.

The fourth and fifth rules establish an IP address that's allowed to download audio and video data from the Internet, but block all other IP addresses from doing so.

ICMP Firewall

If you are experiencing a problem with ICMP traffic simply activate the ICMP firewall and check the types of ICMP packets you wish to let through the firewall. [Make sure to always allow ICMP Fragmentation needed packets.](#) Those packets are required by MTU Path Discovery. If you block Fragmentation needed packets you may experience problems where you can transmit small amounts of data over a connection but large amounts cause the connection to hang.

We do not recommend adjusting the ICMP firewall unless you are very comfortable with what all the different ICMP types are used for. Despite it's bad reputation, most forms of ICMP packets are required for proper Internet connectivity.

10. Web Proxy

The first thing you must decide is whether or not to run individual subnets in proxy server mode or in transparent mode. With regular proxy services, each client is configured to use the CIPAFilter as a proxy server under the "Internet Options" menu in Internet Explorer. Alternatively, transparent proxy does not require each client to be configured, it simply intercepts all traffic on port 80 as it moves through the router.

Disadvantages of transparent proxy:

- No user authentication
- No DNS lookup caching
- No HTTPS Proxy

In non-transparent mode, the CIPAFilter proxy server runs on port 8080 and supports HTP, HTTPS, and FTP proxying. Please be advised, that even though CIPAFilter can properly proxy the HTTPS protocol, it is not possible to virus scan or content filter that protocol because it is encrypted.

Field Descriptions

Transparent Proxy

Ftp and HTTP connections from this subnet will be silently intercepted and injected into the proxy server. Use this option to avoid configuring all your clients with a manual proxy server setting. See above for more information.

Block Downloads

If this feature is checked clients in this subnet will not be allowed to download files. This feature blocks binary file types such as exe, iso, com, cab, tar, zip, rar, etc...

Subnets Authorized to use Proxy Services

Only machines with IP's in subnets listed under this header will be allowed to use the proxy server. Subnets are in CIDR Notation. If 2 subnets overlap the smallest (Most specific) subnet's configuration applies just like in the routing configuration.

Important Exception: The exception to this rule is in the case of transparent proxy. If a less specific subnet has transparent checked the router will catch all traffic from the smaller included subnets as well and force them into the proxy server. This usually isn't a problem however, as these machines can still be configured to use the proxy directly and take advantages of all it's features. However, if the smaller subnet is configured to "require authentication" and a machine on that subnet tries to use the Internet without accessing the proxy directly it will be transparently redirected into the proxy anyway. This will cause the machines connections to be rejected because the proxy server cannot prompt for a username or password when the client doesn't know it's talking to a proxy server.

Require Authentication Feature

The user is prompted for a username and password when they open their web browser (Internet Explorer, Opera, Firefox, Mozilla, etc). The username and password is authenticated against the users on the "User Manager" page or the Windows Domain. Each user's web traffic is logged by username (If web monitoring is active) and can have individual access settings.

Content Filtering Feature

Activates DerbyTech's pornography blocking system on this subnet. Each time a website is blocked the administrator is e-mailed and the block can be recorded in the web monitoring system (If web monitoring is active).

Block Downloads Feature

This option blocks users from being able to download restricted files. Files that are installable, executable or may otherwise contain viruses, spyware or trojans are considered restricted.

Block Flash

This option replaces all incoming flash animations with a simple notice from the CIPAFILTER that flash has been disabled. This is very useful for blocking flash based games.

Blacklist

This check box controls whether or not the CIPAFILTER blacklisting options apply to this subnet.

Authentication Method

This drop down box contains the two "Require Password" authentication methods supported by CIPAFILTER. "User Manager" authenticates against the users on the "User Manager" page. "Windows Active Directory" authenticates against the Windows NT or Active directory domain specified on the IP and Interfaces page.

See the "User Manager" webpage for more information on this authentication method.

To set up Active Directory authentication, choose "Windows Active Directory" from the authentication method drop down box. Create files called proxyauth, proxyfilter, proxydownload, proxyflash, and proxyblacklist in the netlogon share of the PDC containing the word "allow". Access is controlled with file permissions.

- Users with read permissions on "proxyauth" can access the Internet.
- Users with read permissions on "proxyfilter" are not filtered.
- Users with read permissions on "proxydownload" can download restricted files from the Internet.
- Users with read permissions on "proxyflash" can view flash animations
- Users with read permissions on "proxyblacklist" are not blacklisted.

CIPAFILTER checks these files upon each user's first access and cache's the information for one hour. Click "Save and Apply" on the "User Manager" page in the web interface to clear this cache.

The best way to use this feature is to create a few groups that represent the kind of Internet access you want you users to have. For example, a student group might have permission to read proxyauth, but not proxyfilter, proxydownload, proxyflash or proxyblacklist. A teachers group might be able to read proxyauth, proxydownload, and proxyflash but not proxyfilter or proxyblacklist.

Web Usage Reporting Feature

User activity and filter trips are collected for the Web Usage Reporting system to analyze. If this feature is not checked CIPAFilter does not record user activity other than by e-mailing the administrator when the Content Filter is tripped.

Cache Web Pages Feature

Squid web site caching system is activated to reduce bandwidth usage and the time required to fetch websites from the Internet.

Source Proxy from Client IP

Traffic flowing through the proxy will normally appear to have originated from the CIPAFilter as viewed by upstream firewalls and routers. Clicking this check box causes the CIPAFilter to emit the traffic using the source IP address (But not necessarily the original source port) of the client. This feature is not compatible with caching and will silently fail if caching is activated.

E-mail Services

If you already have a mail server, CIPAFilter's e-mail system is designed to act as a proxy and a firewall to protect it from the Internet. CIPAFilter allows you to take full advantage of your mail server's advanced features without the risk of having it accessible to hackers and worms. We recommend placing your existing server behind the CIPAFilter and configuring it with only a private IP address. Change your MX records to point to the CIPAFilter or forward port 25 from your existing MX, and configure your CIPAFilter to route e-mail for your domains to the private IP address of your actual e-mail server.

This will cause all e-mail to be delivered to CIPAFilter, where it will be virus scanned, spam filtered, content filtered, then forwarded on to your actual mail server for processing.

If you don't already have a mail server, CIPAFilter is an industry standard pop3 server that provides a easy to use and painless e-mail system.

Because of the problems with spam in recent years, many companies have become very picky about which mail servers they trade e-mail with. Many unofficial rules have been adopted in a piecemeal fashion across the Internet. If your mail server is configured incorrectly, you may find that most people will receive your messages but for some they arrive marked as spam or not at all. Please allow us to help you through setting up your mail server to be compliant with all official and unofficial guidelines for message processing.

However, if you are an expert, and wish to configure the server yourself, please be certain to comply with the following guidelines. If you don't understand the reasoning behind any of the following, our tech support representatives will be happy to go over it with you.

- Always make sure the IP address pointed to by your MX record reverses to the same name that is contained in your MX record.
- If you are using CIPAFilter for anti-spam do not use secondary MX's.
- Make sure the CIPAFilter host and domain name match the name from your MX record.

To configure CIPAFilter to proxy e-mail for an existing server simply "Add Domain Route" for your domain to route e-mail for it to your mail server's private IP address. To use CIPAFilter as a mail server, add all domains to be served to the "Local Domains" field separated by spaces, check "Pop Mail" above, and add mail boxes in the user manager. Note that CIPAFilter can simultaneously route domains to other servers and process some domains itself.

Also, to use CIPAFilter as an outgoing SMTP server, you must add the subnets your clients belong to to the "SMTP Relay Authorized for the following subnets" list.

Scan Mail for Content Feature

Applies the web content filtering to incoming and outgoing mail messages. If a message is inappropriate a note is sent to the person in your company who was either sending it or was the intended recipient and the message is blocked. This is great for filtering out pornographic spam.

Pop Mail Feature

Activates CIPAFILTER's built in POP3 mail server. Check here, and fill in your domains below under "Local Domains".

Local Domains

When "Pop Mail" is checked, CIPAFILTER will act as a mail server for the domains listed here. Separate each domain name with a space. Do not enter domains here that you intend to route to another internal mail server, use "Mail Routes" below to route those domains.

Notify Address

Informational notices from the CIPAFILTER are sent here. This includes content filter trips and mail errors. This default to administrator@domain, where domain is the domain entered on the "IP and Interfaces" page.

Mail Routes

These entries dictate where CIPAFILTER will route e-mail after it has finished scanning it. If you have a mail server other than CIPAFILTER, enter your domains here to route them to the IP address of your true mail server.

SMTP Relay Authorization

Only e-mail clients using IP addresses from subnets listed here can use CIPAFILTER as an outgoing mail server. The "IP Ranges" entered here are Sendmail style IP ranges, which is just a text match to the text of the IP address.

Subnet	Ip Range
10.0.0.0/8	10.
192.168.0.1/24	192.168.0.
64.215.40.0/25	64.215.40.
12.109.195.200/32	12.109.195.200

Anti-Spam White list

E-mail to or from servers on this list are not affected by the anti-spam system. Enter the server IP, domain names, or subnet here if you have difficulty receiving e-mail from another party. Our anti-spam system works with all standards compliant mail servers, however some older and custom systems may have problems. See "SMTP Relay Authorization" for IP range syntax.

Spam Forwarding

After e-mail has been analyzed by our GreyListing engine some of it will be marked as spam by our modified SpamAssassin. Each message is marked with a number that indicates how likely the message is to be spam. If this box is checked, all messages marked higher than the "Spam Forwarding level" are forwarded to the "Spam Forwarding Address" instead of their original destination.

E-mail Archive

If this box is checked, a copy of every message transmitted through the proxy is stored in the CIPAFilter and can be accessed via the "Email Archive" option under the "Statistics" menu.

11. White list/Black list

The white listing/black listing system allows you to control web access on a site by site basis alongside CIPAFILTER's context sensitive pornography blocking system. In addition to user controlled white and black lists, preconfigured blacklists are provided for categories like gambling, gaming, and image/video search.

Parts of a website like <http://games.yahoo.com> can be blocked as easily as entire sites. The syntax is complicated. Full support for industry standard POSIX regular expressions is provided, but the control over what sites your users can and cannot visit is absolute. Please see Appendix II for regular expression syntax, or simply use the following examples as guidelines.

- Group characters with "(")"
- "*" matches any number of the preceding character or group
- "?" matches 0 or 1 of the preceding character or group
- "+" matches 1 or more of the preceding character or group
- "." matches any single char
- "^" matches the beginning of a url
- "[^/]" matches anything not a "/"
- Precede special characters with a "\" to use them as literals

Example	Description
^http://[^\/*]\.edu/	"^" Matches the beginning of the url. "http://" matches that text in the url. "[^\/*]" matches any number of characters that are not a "/". "\.edu/" matches ".edu/" at the end of the url. The period must be preceded with a slash because otherwise it would be the special "Match any on character" symbol as opposed to the period literal. The effect of this rule is to match all .edu websites.
^http://([^\/*]\.)*?google\.com/	Matches google.com and all google subdomains. The "[^\/*]\." is grouped and made optional so the rule won't match "hgoogle.com", but still matches "google.com" and "www.google.com".
^http://games\.yahoo\.com/	Matches only the games.yahoo.com subdomain of yahoo. If a blacklist entry, users will still be able to use all other yahoo services.

12. Port Forwarding

Port forwarding is a system by which connections to ports on the router can be forwarded on to servers inside your network that only have private IP's. Often times this feature will be used to forward RDP connections from your router to a server inside to enable remote management. When a client connects to a particular port on an IP address belonging to your router, the router instead causes it to connect to the "To IP" on the second port number entered.

In the example below, if your router has the IP 208.16.191.10, and you would like to enable RDP to a server with the address 10.0.0.5 and a server with the address 10.0.0.6, you would create two port forwards like the first two. This would allow you to connect to 208.16.191.10 with the default port to access the first server, and specify the port 4900 when you want to access the second server. In addition, line 3 demonstrates the use of port ranges to forward the 1000 ports starting at 64000 to 10.0.0.4, the "ALL" keyword in the ports field to forward all ports of a particular protocol to the same ports on another machine, as well as the "ALL" keyword in the protocol field that activates 1 to 1 NAT between the "Connections To" IP and the "Forward To" IP. With 1 to 1 nat, All traffic from the "Forward To" address will appear to come from the "Connections To" IP, and all traffic to the "Connections To" IP will be directed to the "Forward to" IP.

Forwarding port 80 or port 22 on your router's only outside IP will make the WebUI or DerbyTech's remote management system unreachable. Try and get a second IP for your router, if this is not feasible be sure there is at least a second private IP address on the router, so you can manage the CIPAFilter yourself.

Protocol	Connections To	On Port	Forward To	On Port	Comment
TCP	208.16.191.10	4899	10.0.0.5	4899	RDP to 10.0.0.5
TCP	208.16.191.10	4900	10.0.0.6	4899	RDP to 10.0.0.6
UDP	208.16.191.10	64000:65000	10.0.0.4	64000:65000	1000 UDP ports to 10.0.0.4
TCP	208.16.191.11	ALL	10.0.0.7	ALL	ALL TCP ports to 10.0.0.7
ALL	208.16.191.12	ALL	10.0.0.8	ALL	1 to 1 Nat of 10.0.0.8 to 208.16.191.12

13. Bandwidth Control

Bandwidth control allows you to keep heavy bandwidth users from washing out all other activities on your network. Bandwidth can be controlled by IP or subnet and is allocated in kilobits per second. Please be advised, that if a user is using their entire bandwidth allotment new packets to them will be delayed or dropped in order to limit them to their prescribed cap.

Users may use up to their max up or down bandwidth at any given time so long as there is bandwidth available. If bandwidth is exhausted, each user is allocated their CIR first, then any extra bandwidth is allocated in ratio with their CIR's. Thus, a user with a CIR of 256 gets twice as much of the extra bandwidth as a user with a CIR of 128, up to that user's maximum bandwidth.

QOS is automatic and each bandwidth queue is handled independently. Within each IP or Subnet's bandwidth allocation OSPF and ACK packets are served first. Then TOS 0x14 and ssh packets (Port 22) followed by TOS 0x10 and 0x0C, RDP (Port 3389) and Citrix (Port 1494) traffic. All other traffic is served from the queue last.

IP addresses or subnets not listed on this page are all lumped together in a single queue which is treated the same way as above, but is de-prioritized as a whole behind everything else. Therefore, IP addresses and subnets listed on this page will have their traffic served first, before any traffic from IP addresses or subnets not listed here.

14. DHCP Server

The DHCP server is very easy to use. Simply check which interfaces you wish to serve DHCP on and enter a range of IP addresses to serve to your dynamic clients in the "Start" and "End" boxes. Machines can be assigned static IP's through DHCP by clicking "Add Static Mapping". The name field is arbitrary and just there to help you keep track of entries.

DHCP Leases shows what machines have received IP addresses since the last time the router was restarted.

15. User Manager

The user manager allows you to add and remove users for web authentication and e-mail services. Each user automatically receives an e-mail box on the router if the router is acting as a mail server. Pornography Filtering, Download Blocking, Flash Blocking and the Blacklist are all optional by user (See the web proxy page for details about these features). UID and GID are the user and group ID's each user belongs to, just leave them default.

Three special accounts exist. "root", "admin", and "guest". The root user controls the password for the router's WebUI. The guest user can access the "Self Service Temporary Password Page", "Anti-Spam Stats", "Anti-Virus Stats", and "Bandwidth Usage Stats" and the online manual. The admin user can access everything guest can, and in addition access the "Librarian Only Temporary Password Page", "Web Usage Reporting", "E-mail Archive", "User Manager", and the "WhiteList/Blacklist". **Note: Admin and Guest cannot access the main page of the router. This means they will have to have a bookmark for or type the link into their web browser for a page they can access before they can navigate using the menus.**

16. Config Save and Restore

This page allows you to easily download the configuration of your router after you make changes. Keeping a copy of your configuration on-hand will allow you to easily configure a new router in the event of a failure or an upgrade. From here you can also revert your router back to factory settings.

17. Remote Console

Remote Console is how DerbyTech accesses your router for troubleshooting. Access is through the ssh protocol. You can disable DerbyTech's access to your router here, but that is not recommended.

18. Statistics

These pages provide you with real time information on the performance of your routers various systems and user activity.

Bandwidth Usage

Clicking on "Bandwidth Usage" brings up the "Bandwidthd" application. This software tracks the Internet usage of all clients on your network. Select an interface under "sensors" and click go to request a report. Custom reports and graphs can be requested by calling special URLs on the CIPAFILTER. Speak with tech support if you wish to embed these reports into other web consoles.

Anti-Spam Statistics

This page shows how many e-mails have been dropped by the first layer anti-spam system. These statistics do not include messages tagged as spam in the "Total Messages Rejected as Spam" percentage, but those e-mails are listed below. These statistics are not stored through reboot, though you may see the old statistics for a few hours after reboot until the router has collected enough information to write out a new set of them.

Anti-Virus Log

Anti-virus engine and signature revisions, as well as a list of all viruses detected and blocked by the CIPAFILTER. Most recent first, numbered in the first column.

Web Usage Reporting

The web usage reporting system is activated on the "Mail and Web Proxy" page. After it is activated, it collects information on every URL visited by your employee's. It will track each user by user name and password if web authentication is activated, otherwise it can only track users by IP address.

19. Appendix I: Dot Notation to CIDR Notation Translation Table

Subnet Mask	Subnet Bits	IP Addresses
255.0.0.0	/8	16,581,375
255.255.0.0	/16	65,025
255.255.255.0	/24	256
255.255.255.128	/25	128
255.255.255.192	/26	64
255.255.255.224	/27	32
255.255.255.240	/28	16
255.255.255.248	/29	8
255.255.255.252	/30	4
255.255.255.254	/31	2
255.255.255.255	/32	1

20. Appendix II: POSIX Regular Expressions

regex - POSIX 1003.2 regular expressions

Regular expressions (``RE"s), as defined in POSIX 1003.2, come in two forms: modern REs (roughly those of *egrep*; 1003.2 calls these ``extended" REs) and obsolete REs (roughly those of [ed\(1\)](#); 1003.2 ``basic" REs). Obsolete REs mostly exist for backward compatibility in some old programs; they will be discussed at the end. 1003.2 leaves some aspects of RE syntax and semantics open; `(!)' marks decisions on these aspects that may not be fully portable to other 1003.2 implementations.

A (modern) RE is one(!) or more non-empty(!) *branches*, separated by `|'. It matches anything that matches one of the branches.

A branch is one(!) or more *pieces*, concatenated. It matches a match for the first, followed by a match for the second, etc.

A piece is an *atom* possibly followed by a single(!) `*', `+', `?', or *bound*. An atom followed by `*' matches a sequence of 0 or more matches of the atom. An atom followed by `+' matches a sequence of 1 or more matches of the atom. An atom followed by `?' matches a sequence of 0 or 1 matches of the atom.

A *bound* is `{' followed by an unsigned decimal integer, possibly followed by `,' possibly followed by another unsigned decimal integer, always followed by `}'. The integers must lie between 0 and RE_DUP_MAX (255(!)) inclusive, and if there are two of them, the first may not exceed the second. An atom followed by a bound containing one integer *i* and no comma matches a sequence of exactly *i* matches of the atom. An atom followed by a bound containing one integer *i* and a comma matches a sequence of *i* or more matches of the atom. An atom followed by a bound containing two integers *i* and *j* matches a sequence of *i* through *j* (inclusive) matches of the atom.

An atom is a regular expression enclosed in `()' (matching a match for the regular expression), an empty set of `()' (matching the null string)!, a *bracket expression* (see below), `.` (matching any single character), `^` (matching the null string at the beginning of a line), `\$` (matching the null string at the end of a line), a `\' followed by one of the characters `^.\$()*+?{\` (matching that character taken as an ordinary character), a `\' followed by any other character(!) (matching that character taken as an ordinary character, as if the `\' had not been present(!)), or a single character with no other significance (matching that character). A `{` followed by a character other than a digit is an ordinary character, not the beginning of a bound(!). It is illegal to end an RE with `\'.

A *bracket expression* is a list of characters enclosed in `[]'. It normally matches any single character from the list (but see below). If the list begins with `^', it matches any single character (but see below) *not* from the rest of the list. If two characters in the list are separated by `-`, this is shorthand for the full *range* of characters between those two (inclusive) in the collating sequence, e.g. `[0-9]' in ASCII matches any decimal digit. It is illegal(!) for two ranges to share an endpoint, e.g. `a-c-e'. Ranges are very collating-sequence-dependent, and portable programs should avoid relying on them.

To include a literal `]' in the list, make it the first character (following a possible `^'). To include a literal `-', make it the first or last character, or the second endpoint of a range. To use a literal `-' as the first endpoint of a range, enclose it in `[' and `.]' to make it a collating element (see below). With the exception of these and some combinations using `[` (see next paragraphs), all other special characters, including `\' , lose their special significance within a bracket expression.

Within a bracket expression, a collating element (a character, a multi-character sequence that collates as if it were a single character, or a collating-sequence name for either) enclosed in `[' and `.]' stands for the sequence of characters of that collating element. The sequence is a single element of the bracket expression's list. A bracket expression containing a multi-character collating element can thus match more than one character, e.g. if the collating sequence includes a `ch' collating element, then the RE `[[.ch.]]*c' matches the first five characters of `chchcc'.

Within a bracket expression, a collating element enclosed in `[=' and `=]' is an equivalence class, standing for the sequences of characters of all collating elements equivalent to that one, including itself. (If there are no other equivalent collating elements, the treatment is as if the enclosing delimiters were `[' and `.]'.) For example, if o and e are the members of an equivalence class, then `[[=o=]]', `[[=e=]]', and `[o]' are all synonymous. An equivalence class may not(!) be an endpoint of a range.

Within a bracket expression, the name of a *character class* enclosed in `[:' and `:]' stands for the list of all characters belonging to that class. Standard character class names are:

alnum digitpunct
alpha graphspace
blank lowerupper
cntrl printxdigit

These stand for the character classes defined in [wctype\(3\)](#). A locale may provide others. A character class may not be used as an endpoint of a range.

There are two special cases(!) of bracket expressions: the bracket expressions ``[[:<:]]'` and ``[[:>:]]'` match the null string at the beginning and end of a word respectively. A word is defined as a sequence of word characters which is neither preceded nor followed by word characters. A word character is an *alnum* character (as defined by [wctype\(3\)](#)) or an underscore. This is an extension, compatible with but not specified by POSIX 1003.2, and should be used with caution in software intended to be portable to other systems.

In the event that an RE could match more than one substring of a given string, the RE matches the one starting earliest in the string. If the RE could match more than one substring starting at that point, it matches the longest. Subexpressions also match the longest possible substrings, subject to the constraint that the whole match be as long as possible, with subexpressions starting earlier in the RE taking priority over ones starting later. Note that higher-level subexpressions thus take priority over their lower-level component subexpressions.

Match lengths are measured in characters, not collating elements. A null string is considered longer than no match at all. For example, ``bb*'` matches the three middle characters of ``abbbc'`, ``(wee|week)(knights|nights)'` matches all ten characters of ``weeknights'`, when ``(.*)*'` is matched against ``abc'` the parenthesized subexpression matches all three characters, and when ``(a*)*'` is matched against ``bc'` both the whole RE and the parenthesized subexpression match the null string.

If case-independent matching is specified, the effect is much as if all case distinctions had vanished from the alphabet. When an alphabetic that exists in multiple cases appears as an ordinary character outside a bracket expression, it is effectively transformed into a bracket expression containing both cases, e.g. ``x'` becomes ``[xX]'`. When it appears inside a bracket expression, all case counterparts of it are added to the bracket expression, so that (e.g.) ``[x]'` becomes ``[xX]'` and ``[^x]'` becomes ``[^xX]'`.

No particular limit is imposed on the length of REs(!). Programs intended to be portable should not employ REs longer than 256 bytes, as an implementation can refuse to accept such REs and remain POSIX-compliant.

Obsolete ("basic") regular expressions differ in several respects. '|', '+', and '?' are ordinary characters and there is no equivalent for their functionality. The delimiters for bounds are '{' and '}', with '{' and '}' by themselves ordinary characters. The parentheses for nested subexpressions are '(' and ')', with '(' and ')' by themselves ordinary characters. '^' is an ordinary character except at the beginning of the RE or(!) the beginning of a parenthesized subexpression, '\$' is an ordinary character except at the end of the RE or(!) the end of a parenthesized subexpression, and '*' is an ordinary character if it appears at the beginning of the RE or the beginning of a parenthesized subexpression (after a possible leading '^'). Finally, there is one new type of atom, a *back reference*: '\d' followed by a non-zero decimal digit *d* matches the same sequence of characters matched by the *d*th parenthesized subexpression (numbering subexpressions by the positions of their opening parentheses, left to right), so that (e.g.) '\([bc]\)\1' matches 'bb' or 'cc' but not 'bc'.

SEE ALSO

[regex\(3\)](#)

POSIX 1003.2, section 2.8 (Regular Expression Notation).

BUGS

Having two kinds of REs is a botch.

The current 1003.2 spec says that ')' is an ordinary character in the absence of an unmatched '('; this was an unintentional result of a wording error, and change is likely. Avoid relying on it.

Back references are a dreadful botch, posing major problems for efficient implementations. They are also somewhat vaguely defined (does 'a(b)*\2*d' match 'abbbd'?). Avoid using them.

1003.2's specification of case-independent matching is vague. The ``one case implies all cases" definition given above is current consensus among implementors as to the right interpretation.

The syntax for word boundaries is incredibly ugly.

This page was taken from Henry Spencer's regex package.